Department of Homeland Security
Data Privacy and Integrity Advisory Committee

OFFICIAL MEETING MINUTES

Tuesday, March 7, 2006
Ronald Reagan Building International Trade Center
Polaris Room
1300 Pennsylvania Ave, N.W.
Washington, DC 20004

AFTERNOON SESSION

Ms. Sotto: All right. Thank you for returning for the afternoon session and thank you to the panel for being seated. Our afternoon session will focus on operating within an information sharing environment and our first speaker is Jim Williams.

Mr. Williams is the head of the U.S. VISIT Program. VISIT, for those of you who don't know, is the U.S. Visitor and Immigrant Status Indicator Technology, more commonly known as U.S. VISIT. U.S. VISIT is a critical border management program that allows for the collection of point of entry and exit information on visitors to the United States. Mr. Williams, the floor is yours. Thank you.

OPERATING WITHIN A INFORMATION SHARING ENVIRONMENT;

MR. JIM WILLIAMS, DIRECTOR, DHS US-VISIT
MR. SCOTT CHARBO, DHS CHIEF INFORMATION OFFICER
MR. LUKE MCCORMACK, CHIEF INFORMATION OFFICER, US IMMIGRATION AND CUSTOMS ENFORCEMENT
MR. FRANK DIFALCO, DIRECTOR, HOMELAND SECURITY OPERATIONS COORDINATION

Mr. Williams: Thank you. Good afternoon, everyone. Thank you for having me here today to talk about the U.S. VISIT Program and information sharing and I have to say before I start it's been a great partnership with out Chief Privacy Officer, Maureen Cooney, and her office from day one and her predecessor, Nuala O'Connor-Kelly. Let me talk to you a little bit about the purpose of the U.S. VISIT Program and how we relate to privacy and what we've accomplished so far. The U.S. VISIT Program is actually a mandate of Congress from 1996 called the entry/exit system aimed at combating illegal immigration. Post-9/11 other laws were passed mandating the need for this entry/exit system aimed at combating terrorism. All of those laws also said implement this program in a way that does not adversely impact legitimate trade and travel. As this program was named U. S VISIT by our former secretary it was done so to reflect the fact that the United State is a welcoming nation and will continue to be so for all countries. And what we've done so far is first of all we establish our goals and we live, breath, eat, and sleep these goals. And they are to enhance security for citizens and visitors. We want people to come to the United States and we want them to be safe when they come here. Secondly, as the law mandated, we wanted to make sure we facilitate legitimate travel and trade. We know that 99.9 percent of the people who come to the United States come here for legitimate reasons to study, travel, seek medical help, do business, see families, and we want those people to come. Our third goal is to ensure integrity in our immigration system. As the President said in his State of the Union Speech two years ago, we want people to come to the United States but we want to know why and did they leave on time. That's ensuring integrity in our immigration system. Our last goal is to protect the privacy of our visitors and that's something I know that is near and dear to your heart. What the purpose of the U.S. VISIT system is, is to be able to record the entry and the exit of foreign visitors to the United States but it's also, as Congress mandated in its 2000 Data Management Improvement Act regarding the entry/exit system, was to make sure that we could aggregate information and make it all across the immigration and border management spectrum and make it accessible to decision-makers. So in effect we're building an information system that gets the right information to the right people at the right time to make the right decision. And just to give you an idea of what we've done to date, since we started the program in January of 2004, we have since that time processed people through air, land, and seaports over 51 million people. And what that means is for people is we have been able to take their biometrics, their two digital index finger stands and a digital photo of those people coming in through our ports of entry and sometimes in between our ports of entry and be able to check those biometrics to see if they are who they say they are and to be able to see if they're also on a watch list. What we also did with privacy, and I believe as Maureen does about privacy, is privacy is not something that you think about later, it's something that you integrate from day one, and what we're trying to do is trying to transform our immigration and border management systems to make it easier for people to travel, to receive immigration benefits, and make it harder for the bad people to do the same thing, to be able to come up and take advantage of our systems to exploit them. We believe we have to, as Maureen has said to you, integrate privacy from day one. And what we're trying to build is not just simply an information system but it's really trying to transform our immigration and border system into a total solution that combines the right policies, the right infrastructure, the right people, the right information technology, and the right business processes. Privacy intersects with all of those different parts of the solution. What we did work with Nuala O'Connor-Kelly was even though the privacy act and the government act does not strictly speaking apply to foreign visitors we decided from day one to apply the principles of the privacy act. And we did so because it's the right thing to do but also because as foreign visitors come to the United States, not only do we want them to feel safe in coming to the United States, we want them to feel safe in what we're doing with the information we're collecting. We also believe, as Nuala used to say, that what U.S. VISIT does is it protects your privacy. As we take people's biometrics, we make sure that nobody else can assume their identity. We know that there's certain parts of Washington, D. C. where you can drive along the street and in your car and you can do a signal like this and that means for $25.00 or so you want to buy somebody's identity. There's parts of D. C. where you can do that. We knew that you could buy a fake passport for a $1000 or $2000. What we've been trying to do is introduce biometrics to be able to protect the good people who are trying to come to our country and make it easier for them to do so and make it harder for the bad people to do so. We are engaging in other activities as we move on into other deployments as part of U.S. VISIT that are sensitive to privacy concerns, and I'll tell you what some of those are. Number one, there is a mandate for countries from the visa waiver program, that's 27 countries, England, France, Germany, Japan, Australia, those people today can come to the United States for up to 90 days for business or pleasure. They don't need to go by the State Department first to get a visa. They can come here on just a passport. That is susceptible to exploitation by people who want to do us harm. And I'd like to stop and just quote Dr. Zelikow who's a counselor to Secretary Rice who is Executive Director of the 9/11 Commission when he talked about what he learned through that experience. He learned that the terrorists are much like people who are in a submarine. When they're in a training camp somewhere, they're standing deep underwater but in order to do harm they have to come up and in order to come up they have to travel and understand our immigration and border management systems, and they study those and focus on them exclusively. They're always looking for our vulnerabilities. Having people who come to the United States on a visa waiver program who do not have to go through a State Department interview or at the State Department today they take the same biometrics that we do, ports of entry, and check against our databases and since they started doing that fully in October, 2004, they've had over 15,000 biometric hits. What we're doing with those people who come here with just a passport is requiring that they put an integrated circuit chip in their passport that contains their biometrics of at least a digital photo. And then we use that digital photo to make sure, again, this person is who they say they are. When their passport will be read, and we're testing this in San Francisco Airport right now, we'll test to make sure as we can extract that photo from the chip, we'll look at the person in front the inspector, the CBP officer, and make sure it's the same person. So that's introducing biometrics to protect people's identity, to protect us from people who want to do us harm in visa waiver countries. At our land border sites we're also looking to work with a partnership with the State Department and all parts of DHS on implementing something called The Western Hemisphere Travel Initiative. What that requires is by January 1, 2008, if you want to cross from Mexico and the United State or Canada and the United States, if you're an American citizen today you can cross with nothing, no identification whatsoever. In fact, some people say the only determination of whether you're a terrorist is how good is your American accent. What we want to be able to do is implement the law, the Intelligence Reform Terrorism Prevention Act, Section 7209 that said on January 1, 2008, Canadian or U.S. citizens who are coming into the United States through our land border crossings must either have a passport or alternative travel document. We are looking to work the State Department to develop an alternative travel document, one that we're emphasizing the need for using radio frequency identification technology. Using RFID, much EZ Pass, where we would have people carrying a wallet-size card that would have an RFID antenna in it that would do three things that we don't do today at the land border crossings. First of all, it would allow for that vast majority of people who come in buses, vehicles, on bicycles, and on foot, we would be able to read that RFID and the information from that antenna which all that would be in there would be about a 60 digit long serial number that would point back to a database. But that database would then allow us to put the information, preposition it, on the officer's screen. So if you're driving up from Tijuana to San Diego in a car, 30 feet before you reach the officer's booth, it would read that information, it would put the information up on the officer's screen thereby enhancing security and allowing him to make a more facilitated inspection, hopefully speeding things up, and it would also -- number one, it would be able to preposition the information on the screen. Number two, it would record the entry of people which we don't today so we don't know everybody who's in the country. And, number three, we hope it will allow us in that few seconds time-frame from when it's read to when it goes on the officer's screen we'll do a watch list check against it. And that's something we know as we try and implement these solutions and design, we need to work closely with a lot of people to make sure that we integrate privacy as part of that total solution. We take very, very seriously our requirements around privacy and it's not just what we do in privacy, it's the perception that we convey. I often talk about privacy and refer people to the National Spy Museum where there's a survey on the wall, how many Americans think that the U.S. government keeps a secret database on them? And answer is 67 percent. So I always say if Americans think that what do you think our foreign visitors think about how we treat their information? We do share information appropriately with intelligence and law enforcement sources. That's part of our job is to enhance security but part of our job is also to protect that privacy so people feel safe in providing us that information, and we can help protect their identity and protect their security. With that I'll stop and open up for questions.

Ms. Sotto: Thank you so much. We appreciate your joining us. Mr. Palmer.

Mr. Palmer: Regarding this RFID capability, perhaps you can help me understand something here. The RFID chip is in some sort of document that they've been given, issued by some trusted agency, and this RFID chip contains a number that you use to look up in some database somewhere. Particularly in the bus load version, how do you know that the passport or whatever the device is imbedded in is actually borne by the owner and not just tossed in the bus or carried by someone else?

Mr. Williams: Well, on the bus it's more difficult. Generally, people on buses today have to get out. They have to get off the bus and go in and be processed inside. What we're trying to build actually is something where we could read this both for entry and exit. On entry, the people on the bus in the short term would probably have to get out. What we're looking to do is advance technology so someday that officer could get onto the bus without people having to get off and have the ability to read the information much as we would do with the biometric passports and put the picture up on the screen with a biographical watch list check. That gives them a great degree of assurance when they're doing their interview or inspection. We don't have all the answers here but let me tell you where I would like to be if we could push a button with technology. I would like to not just have this be something that transmits the serial number but it would also be able to for foreign visitors -- what we really would like is a card where somebody could press down a biometric, because we're trying to record entry and exit in. If somebody, if this has RFID in it and this leaves the country, all I know is this left the country, I don't know that I left the country. But if I put down a biometric on this, and this technology exists today, where you could put down a sensor and then I could record the, check the database, see if the fingerprints are on a watch list, that gives me a more secure identification of the person. But what we're doing when it's not a bus is if you can take four people in a car coming from Tijuana to San Diego, it would actually pop up on the screen all four of the people's photograph. And that actually exists today in our trusted traveler programs. And then the officer would look at all four of those pictures, look at the four people in the car, and then say okay now I know who you are, I've recorded your entry, I know you're not on a biographic watch list. Buses are tougher and right now people do -- everybody gets off the bus. But what we do with pedestrians though is when you walk in the building just almost like walking into a department store where they know if you're leaving with something, that information that's in the card is read as you walk in so that by the time you get up to the officer's station, if you're on a bus and you have to be processed through different lines, they read the call and all of a sudden the picture pops up, the name pops up, and what we hope to do is be able to have that watch list check done, too. Does that answer your question?

Mr. Palmer: Yes, it does. I have another followup, if you don't mind.

Mr. Williams: Sure.

Mr. Palmer: You mentioned biometrics earlier, fingerprints. Have you any idea what the false accept rate has been? You certainly -- I suspect you won't have any idea about the false.....

Mr. Williams: Positive?

Mr. Palmer: Yeah, the false positive.

Mr. Williams: I can tell you, our false positive rate today is about .1 percent which is still high. And let me explain, what that means is when we think -- when somebody puts down their finger scan and then it's checked against the database, it's checked to see are they on a watch list, where we think it's a match they then go in the secondary for processing and it's not a match, meaning they weren't that bad guy, they were innocent, that's in .1 percent of the cases. That's too high for us because .1 times a large number is still a big number of people who are innocent but who are sent to secondary. One of the things we do today is when that appearance of a match happens, immediately those fingerprints are sent to a biometric support center and we have two of them that operate, one in my building in Rosslyn, one in Otay Mesa, California, human fingerprint examiners usually former FBI examiners look at that very carefully. And these people have extremely well-trained eyes and they can tell within -- and our average is about three minutes or less whether that really is a match or not. What we're moving towards though is moving as the

Secretary said last July 13th, we're moving to take 10 prints on enrollment the first time we see you. Because what that allows us to do is to be able to check against more information and our degree of accuracy we hope will just shoot up. Well, we know it will. We know it's going to go up. And it's like taking ten people in a room and saying oh I want to describe one of the people. Well, it's easy to do it because ten people have very much differences. Put 10,000 people in a room and then you have to give more identifying characteristics. And that's what 10 prints does for us. And we have plans with the State Department to move to 10 prints on enrollment. Enrollment means the first time we see you we want to be able to take 10 prints. The second time and every subsequent time what you're after is verification. We'll probably be able to make do with one, two, or four prints. But that's how we're going to even lower what I think is already a low false positive rate. And also our false accept rate. I mean, that's something we're also very concerned about, too.

Mr. Palmer: It's a little harder to measure.

Mr. Williams: It is. How do you know when somebody got through who shouldn't have?

Ms. Sotto: Thank you. Mr. Harper.

Mr. Harper: Director Williams, your testimony reminded me of a question I received the other day. I operate a privacy website that is available the world over with information and it really was just about a week ago I got an email from a Briton who has come to the U.S. I assume through the U.S. VISIT Program had given a biometric, I think fingerprints, his holiday is now over, some months I think, and he says and it's gnawing at him that his fingerprints are now in a U.S. database. How can he get the fingerprints expunged from the database? I may have told him I would try to find out and if you can make me a truthteller in that respect I'd appreciate it. An interesting problem. After a year where someone has not returned to the country, do the records -- are they destroyed, is there a way to get them expunged?

Mr. Williams: Well, what we've also tried to do is we've implemented the principles of the privacy act is answer all those basic questions in a very public and transparent mode by publishing our privacy principles, publishing our system of records notice, and answering those basic questions, what information you're collecting, how long are you keeping it, who are you sharing it for and for what purpose. How we keep the information, historically, in this biometric system the prints I believe were kept for 75 years. And let me tell you, I think there's a good reason why. We're revisiting that but it will still be a lengthy period of time. Right now U.S. VISIT applies to anybody over the age of 14 and under the age of 79, and your British person that you met may not come back for a year but he may come back three years from now. And we want to be able to compare those fingerprints to see if they're -- it's the same person who came through before. We don't want him coming back and trying to use a different identity. So we will keep the fingerprints for a long period of time so we would not agree to expunge those records.

Ms. Sotto: Thank you. Mr. Leo.

Mr. Leo: .....Secretary addressed us, but I did not have a chance to ask this question but it has a lot to do with our subsequent work in identity management and privacy and you are at least at the forefront of identity management with the U.S. VISIT Program and Western Hemisphere, but we also have other programs in the department including the identity management under HSPD-12 for credentialing, we have the TWIC card, the transportation worker identification card, guest worker program, border crossing, REAL ID, et cetera, and earlier there was an initiative which I lost sight of which was a screening coordination office. How does the Department of Homeland Security look holistically at all of this identity management so that there's some sort of theme and not just in terms of privacy but cost-effectiveness, interoperability, and all of this, and I would appreciate it if you could address a little at least of what you know about what the department may be doing to coordinate with your program and others this identity management and credentialing issue. Mr Williams: Well, the Screening Coordination Operations Office, the

SCO it's called, that was an office the Secretary advocated for the creation of to look across many of these programs and I know that they're hoping to get a leader for that office by the end of this month. That's what Deputy Secretary Michael Jackson told me about two weeks ago. How we coordinate, one of the things we do in our office is look to on many of the screening initiatives and it's really party under, I guess a delegated assignment by Scott Charbo the chief information officer could probably talk about this, is looking at the screening portfolio information technology systems and how they should interoperate. We also work closely with our policy office because when we looked at some of the biometrics programs a while back for Admiral Loy we looked across the department. He asked us, U.S. VISIT to do this, and we found there were many different biometrics programs and what we really need to do is bring them together from about four different perspectives. One, is the business process perspective of what is it you're trying to accomplish, and we don't have to unite all of those things. Frankly, if the Coast Guard is going to take the DNA of their servicemen that can be a separate database. However, if we're screening and what we look at is across the immigration and border management spectrum where at the State Department somebody applies for a visa, that person then comes into a port of entry at Dulles Airport. That person then wants to adjust their benefits with citizenship and immigration services or that person is somebody that immigration and customs enforcement -- we've been trying to unite identity management across that immigration and border management spectrum. But also looking at it from several perspectives, one, is business process. One is having harmonized policies as appropriate, looking at the business process policies, looking at the information technology, trying to set the standards like in HSPD-12 which is the identification credential for government employees and government contractors, how should those be similar to a transportation worker identification credential, the TWIC card. And then, lastly, just from an R&D perspective as we're always trying to improve things in the area of identity management, what we've done is tried to unite with other agencies. For example, when we want to use a mobile biometric device, if you think about it the border patrol with somebody standing in front of them in the middle of the desert or a war fighter standing in front of somebody in the Iraqi desert or Coast Guard with somebody 400 miles off-shore or somebody standing at general aviation at national airport, all that's about being able to identify that person and are they somebody who is at risk. What we're trying to do is unite the policies, the information technology, for us at least across the immigration border management spectrum but then build out a solution that is reusable by other agencies. The Screening Coordination Operations Office will certainly help do that but I think some of the work that Scott has chartered different components of DHS to work together on is also helping that. We also work closely with our policy office to make sure it is truly harmonized policies as appropriate. So does that answer your question, Joe? I'm trying to protect against the evil identical twins out there. Joe and I have both identical twins.

Mr. Leo: I don't think that my colleagues knew that. [Laughter]. I'd send him in every other meeting.

Mr. Williams: We both happen to be the.....

Ms. Sotto: We knew you were fascinating.

Mr. Williams: We both happen to be the left-handed, mirror-imaged twin, too, which is pretty unique.

Ms. Sotto: Thank you. Reed.

Mr. Freeman: Thank you. Not twins of each other? [Laughter]. With respect to RFID deployment by the private sector or the government, many worry about data leakage or unauthorized access by surreptitious interception through compliant readers. Is this something that you're worried about or taking into account?

Mr. Williams: We're extremely worried about that. First of all, what we're trying to with RFID is make sure that if you want to protect the information the best you put it in the database don't put it on the card itself. And let me talk about two different instances. One is where it's a U.S. issued document. We want to put the information in the database so if anybody could ever read it all they'd read is that very long serial number. Where it's a document issued by another country such as a French, Japanese passport, what they're doing and what the United States is doing is they issue what's called their E-passports is they're using something called basic access control. There was a concern that if I had my passport in my pocket somebody with a powerful reader could read that chip and then know that I was an American. The steps that have been taken to protect from that which most countries, United States and others are moving towards, is called basic access control or BAC. What that means is when you open up your passport today and you see those optical character lines at the bottom, that's called the machine readable zone. And what basic access control will do is say the only way you can read that integrated circuit chip is to first read through an optical character reader that machine readable zone. That then becomes the key to unlock the information that's in the chip. So that means nobody could walk by with a reader and just read that information. The only way they could read it is if they put it down on a glass reader to read the OCR optical character recognition machine readable zone. That then would unlock the information that's in the chip, you could read it. So nobody could walk by you and read it. Using the U.S. issue travel documents, again, what we're trying to do is take the biographic and biometric information and put that in the database. But still if you had a 60 digit number and somebody knew your 60 digit number they may not be able to know who you are because they wouldn't be able to hack our database. But if they knew your number they might say well I knew your number was, you know, 1 through whatever and then they might be able to say well is that you. We're looking at things like putting a some type of -- I think I might even have one here, maybe I don't -- you could put it into a metallic shield where the card would go into it so therefore you couldn't read that while you had the card inside of that, much like what you put your ATM card inside, but use that as a shield to reader. If I could push a button, again, I would prefer there's technology starting, coming along, where you have RFID in a card you can actually press an on/off button. And we wish we had that. We do have a job to do right now to enhance security now and to meet the requirements of the law in terms of the Western Hemisphere Travel Initiative to get something out there in the cards, but I think we want to do everything we can to protect the privacy and that's not a job that's going to stop. As the technology gets better, and I believe this, as technology continues to accelerate, and I'm actually in the middle of reading a fascinating book on this called The Singularity is Near talking about the, you know, the technology improvements that happened in the last century, they're going to happen in the first 20 years of this century and then those first 20 years that's going to happen in the next 10 years, in 2010 -- 2020 through 2030. We've got to continue to be able to develop the technologies along with the business processes and practices and policies to allow privacy to move in locked step with that. And that's what we're trying to do. So we're very concerned about that and we know that there's concerns out there in the community about this. And, again, we want -- what we want to do is provide a tool that helps that officer know whose in front of him or her and be able to protect that person's privacy. But also if you look at our land borders we want to facilitate things. If you've ever been out to some of our busiest land borders and I know you all have, you look at the needs of the 21st century and these look like economic choke points from the 20th century. I mean, there's cars and trucks waiting to do business with the United States backed up for miles, creating pollution. We want a way to be able to facilitate people while still protecting their privacy and frankly make North America more competitive. Because if you have to wait in line hours and hours just to deliver goods from Maquiladora in Mexico, it may be faster to bring it in, you know, fly it in through China. We just want to remain competitive but at the same time protect people's privacy. So we are concerned about it.

Ms. Sotto: Thank you. I would ask the rest of you to please hold your questions for Mr. Williams and let's see if we have time to come back after the rest of the panel -- if the rest of the panel doesn't mind, I'd like to push the time back a little bit and eat from -- our discussion of the subcommittees about 15 minutes or maybe a half an hour depending on how the rest of the panel goes. If you all have time to stay I think everybody is quite fascinated by this discussion. Thank you. Next on the panel is Scott Charbo. Mr. Charbo was nominated in June of 2005 to be the Department of Homeland Security's second Chief Information Officer. Prior to coming to DHS Mr. Charbo was the Chief Information Officer for the U.S. Department of Agriculture where he was responsible for overall management of USDA's information resources and IT assets. Mr. Charbo, Thank you for joining.

Mr. Charbo: Thank you. It's a pleasure to be here. I started on July 5th and the CAT scan was on July 6th and that passed so I'm still here. Actually I think it's a good time to be at DHS because I think we actually have some things in front of us that we can achieve. Let me kind of give you a focus of some of the five things that we've tried to focus on from the CIO shop as it pertains to overall transformation of some of the department IT assets as it relates collaboration and privacy and information sharing. We've sort of aligned those in five large buckets, if you will. One of those is it relates to enterprise architecture and trying to align that with our systems and also to the budgets. You know, a core facet is the system's inventory that we have and then the components of that. One of those are people that access it and data that resides in these systems. We've published the first systems inventory just early in last calender, or late in last calendar year and we are not mapping lots of our activities towards that. One of those are architecture and we'd also like to know how that aligns to a budget which is usually how items are appropriated to program areas or budgets. You're never quite sure where those things line up but we see a value in keeping those aligned. As budgets are reduced, what systems are impacted by that? Will they be maintained? Will the security infrastructure of those systems be maintained? That's some of the value we see in bringing that triangle together of systems with investments with the budgets, et cetera. The other area we have going on, one of the second of the five, is our infrastructure alignment. Four key areas of that is a data center. We currently have 16 large data centers that we maintain. Not all of those have complete disaster recovery functionality to those so we are focused on bringing together a data center environment that we can consolidate those into two active/active with proper disaster recovery, support to the systems that we house in those data centers, and also some common operating environments around those to maintain the integrity of those data centers. We have an email consolidation. We have thousands of email servers, lots of little databases, lots of these are legacy issues from the consolidation of DHS and we have a project that we started to bring that together. We have a global address list now which enables us to communicate to all employees for really the first time in an email environment without building those lists yourselves. Third area of the infrastructure is our network. It's a critical aspect of our infrastructure project. We're moving towards one net. We have many wide area networks. Those networks are being consolidated into our core platform of one net. We do now have a central NOC-SOC for the first time which we're proud to say for the department where we are able to monitor that environment and view the packets, view the routers, view the applications, how much of the application is moving through the network, and that data's actually just been formed and we're in the process of mapping the wide area networks onto one net as we speak. And the other main bucket in the infrastructure in a help desk support of brining that together to serve as the users of those other infrastructure. We're focused on our security score, our FISMA score. We've made it easy for our security officer, he has one performance goal. That's FISMA. It's getting a 100 percent certification and accreditation compliance. Big part of that is privacy impact statement for the systems, again, keeping that systems inventory our baseline. It may grow, it may shrink, that's fine. We want to know what happens to those systems when it grows and when it shrinks but we also want to ensure that they've been certified and accredited. I started, we had roughly 20 percent of those systems certified and accredited. It's an F. It's been an F. We are now at about 60 to 65 percent of C&A completion in just a few months. So when you get relentless and you put some focus to it, you actually can move progress in that area. So we're mapping towards a 100 percent certification by the end of this calendar year. Is that 100 percent a magical item? You know, we'll be bouncing in the high 90 percentages because systems will come on and off. I think what we'll find is we'll do some IV & V, find some areas that we need to remove the accreditation and do some shoring up but that's managing your inventory. That's managing your environment. And that's the way it should be. But we shouldn't be at 20 percent. We want to get those systems accredited so it's a major priority for us. The fourth area is energizing our information sharing, and I'll come back to that aspect, but it's a major part of extending our information to our state and local partners. A lot of that is under, the titles you're familiar with are Fusion Centers, across programmatic areas so that we're looking at the right information at the right time and we have the proper security assurance bundled around it. And then just one that's sort of near and dear to me. It's, you know, we really need to try to get focused on projects that deliver some actionable outcome. We have a lot a projects that sort of start and they don't go very far so, you know, from our focus we want to either stop and end those and retire them or move them into operations and decide how to continue and move those projects out. So from those areas of how we bring that together for collaboration and privacy and information sharing, we start at the architecture. It's simply mapping where you are today on an as-is and where you want to be and build those processes of how you do that. A large part of that is a data architecture, data standards, and policies as Jim mentioned in terms of people screening. We have stood up an extension of our CIO council that's focused primarily on people screening. We know we have 87 or so processes in terms of analyzing or screening of people. We know we don't need 87 processes. We can reduce that work flow down and service the DHS clients or customers as well as components with fewer processes to that and bring greater assurance and stability to the systems into the data. We've brought the focus of the screening across the four or five components that enable 90 plus percent of the screening activities and then we bring those to the architecture through the council as full. We've also stood up a case management steering committee. Luke's actually the chair of that and Scott Hastings the chair of the people screening one so we try to bring some focus to those areas where we want to see things move from projects into some real actions. We've also focused on an intelligence information sharing committee as well that's sort of within our information analysis group. So it's within building that architecture. The other area that we want to assure in terms of the collaboration environment is the security aspects and it's tough to make that up. Right now I'm on a remediation process. We did not have our systems accredited. Again, we can blame that historically but the fact is, is where we were is where we were and we need to fix that. So we're in the fix process. But at the same time, we need to change that culture and build those processes within the programs themselves and that's key as we begin to build more information sharing. From the collaboration side of things, you know, our -- it's interesting coming from, you know, I'm a third twin with Joe coming out of agriculture. He was number two, I was number three. That's how we like -- number two, got you. The collaboration area, if you really look at that space, it's a lot of collaboration rooms. It's a lot of I wouldn't say chat but it's posting of content that's unique to a subject area. And there's administrators to those subject matters or areas and they allow people into that room by proxy or by extending an ID and password and keeping the rest of the communities out. And there's quite a proliferation of that and a lot of information sharing is actually done in that process. So, you know, it's breaking -- it's not an IT issue. I mean, the fact that we can create these collaboration rooms rather quickly, it's not an IT issue, it's a culture issue. So, you know, we are really engaged with the business side of that of trying to break some of those barriers down. And it's simple questions. I can extend you a right into this data or I can extend you a right into this case management file, but then what are you going to do? What are you going to do with that information? How do we assure -- I can assure that you have a background check and I can assure that you had the right clearance but this may have some legal aspect, it may be an active case with some evidentiary chain, so how do we build that assurance around that you are not going to do something that would damage our case or maybe Luke will touch on something like this. But those are the types of barriers that have stood in the way of information sharing and collaboration in the past. So we're looking at ways of building that assurance around the system, around the data, around the individual and matching those up to provide greater assurance. So that brings us into, and really the last thing I'll say is around identity management and we've already touched on that with HSPD-12 I guess is the label that we've put on that. We have the standards in place. Those are the FIPS code and HSPD-12 in terms of an initiative that has the background check standards so that we have some assurance that background checks are being done on individuals consistently, that I can trust the way that you are doing a background check, you can trust the way that I do a background check. The second part of that is the issuance of a standard card with the biometrics, the electronics, whatever. It's chocked full of those, of the gadgets on the card so if I can't get into it after I've been issued that I'm in real trouble because there's all kinds of things on the cards. So we have that ability to do a variety of methods in order to provide access to it. The last part of is which personally I think is the tougher part, it's that logical access side to the applications and such. And that's still in its infancy so, you know, we can work from one application to the next but in terms of broadening the application and access to it via an HSPD-12 type environment and that PKI environment or however we structure it, it's still in its infancy and there's a lot of work to do in terms of mapping and matching up all the little databases that currently exist out there. With that, I'll close and if you want to wait for questions to the end or I'll take those now.

Ms. Sotto: I think we'll take them now and see how we are on time. Thank you so much for your comments. Mr. Hoffman.

Mr. Hoffman: Mr. Charbo, thank you very much for spending this time with us. I'd like to start off by commending you. From what I understand from staff as we've been looking into the privacy impact assessment process, the FISMA C&A process has been absolutely instrumental and I think in our early analysis we really see the privacy threshold analysis and then the PIA as the bedrock of any privacy compliance program. I'm wondering your thoughts on how that could even be taken to the next level, assuming that the department had the resources to do it. I think from incorporating similar, a similar program in the private sector my, one of my learnings was that it needed to get, the assessment needed to be done as early in the development process as possible to get people thinking early on. And I think FISMA C&A as I understand it is probably about midway through development process. I'm wondering your thoughts on how could the two organizations take this even further and get the individual programs thinking earlier about the privacy and the information security issues.

Mr. Charbo: My preference wouldn't be to build that from the department CIO point. You know, I think we've budgeted in order to try to maintain some processes to better standardize the FISMA and the privacy impact as it pertains to active operations. I don't manage the privacy program but I do have responsibility to assure that the systems in operation meet those standards. We would rather see that being pushed down into the components where those operations are active, running, et cetera. So if there's added resources to come, we would like to see those down in the components to assure that they're actually getting those processes done. I wouldn't see that adding to my budget, from a budget perspective. From the -- I think a big issue is -- the first big bucket I mentioned was alignment of our systems to our investment processes. And right now those are all different people so we have FCIO's in components, we have security people in components, and we also have investment people in the components who sort of build the investment portfolio. Sometimes that involves CIO in certain components, sometimes it just involves the financial officer or the budget officer. And it's that integration that we're going to need to get to in order to better assure ourselves that within this budget category and then how it aligns up in an appropriation that everything's matched to assure that the security systems or the security processes within that component are budgeted, they're there, and then they're actually carried out. Then we can hold the CIO's accountable to assure ourselves that that work's getting done. Within my budget we maintain a very small margin in there that if we need to do some remediation with a component that we're able to step in and do that. To this point, just by keeping a score card, good communication, I think we've seen a move from the 60 -- or the 20's into the 60 percent in just a few months and we will get it there. We'll go back and look at it, we'll revisit it, but in order to get in front of the problem as you suggest I really think it's that alignment of the budget process, the appropriation process and knowing what systems are where because they're just not -- I can look at a 300, I can look at a 53 but those aren't projects, those aren't systems, those are investment documents. And bring those together it's not quite there yet and I'm not talking DHS. I'm talking most agencies are that way. I know it was that way at agriculture because I came from there.

Mr. Hoffman: Thank you,.

Ms. Sotto: Thank you, Mr. Charbo. Joe Alhadeff.

Mr. Alhadeff: Thank you. It's kind of fitting that I get called after David because I'm going to ask his question in a slightly different fashion. And the first thing I'd like to do is get a little bit of clarification, when you said 60 percent have a certification on the system, does that also include the 60 percent have gone through a privacy impact analysis.

Mr. Charbo: What we've done is we've stood up sort of couple of systems. One of those is to provide agencies a mechanism to see what they need to do in order to move towards compliance and it's the formulation of the 11 or so documents. One of those is a privacy impact assessment. Until those documents are actually placed into our repository and each of those documents are actually reviewed by members of my staff or contractors on our staff, an ATO, authority to operate letter is not actually accepted. So our 60 percent represents where we are in terms of getting to our 100 percent certification by the end of the year.

Mr. Alhadeff: Okay. And then knowing -- I mean I agree with you on the fact that you have a piece of the pie as it relates to privacy impact assessments and what you can do with them especially before a project gets to a system, but there's also the concept that even with systems not all of them would be entirely visible to something like the privacy office. And operating as a CPO in a private sector company, one thing that's immensely useful to me is kind of an eyes and ears concept where relying on the technology people to let me know when there is a system that they may not be the only ones who are responsibility for it but because they have an operational hand into a good number of the systems, they often operate as kind of the early warning system in terms of threshold analysis and things of that nature. So I was wondering if there's anything that you can do devolving through the people in your reporting chains to perhaps help be more of the ears, the eyes and the ears of the privacy office in terms of getting them involved in places they need to be involved and making sure they have a complete inventory of the systems they need to be aware of.

Mr. Charbo: I think how you describe it is actually how it is. So the inventory wasn't accepted until those CIO's, those IT folks in the components accepted it. Once we've documented that inventory then we went to the process to assure ourselves what documentation was done on those systems. So we also do -- you know, we try to integrate this as I see investments for procurements, we look at that procurement and say what system is this, is it in the inventory? I look at fedbizopps. Right? I'm an old IT private sector hack as well so, you know, I know there's a lot of activity that goes on in fedbizopps. I look at that. As I see a procurement, one that we may or not have been aware of, we as the question is this in the inventory? So everything goes back to start when I see a document maybe even a hearing that we are able to review the notes or some document that's going up to the Hill, the GAO, the IG, we look at those. If we identify a system, question we ask is, is it in the inventory? If it's not in the inventory, then it goes back to the technical folks and say what is this, why isn't it in the inventory? And then we start building the documentation that's on that if it doesn't already exist.

Ms. Sotto: Thank you. Mr. Barquin, you have the last question.

Mr. Barquin: On the theme of twins, actually this committee really sometimes I feel are twins separated at birth and the cry for one of those twins not to disappear into a world of malnourishment. And that's the integrity, the data integrity side. There is a privacy community out there that, of course, wants to know what we do on the privacy side but I feel that integrity, the data integrity is just as important. It is a twin brother or sister in the process and I suspect that you, Mr. Charbo, if anyone, has at least been thinking about the data integrity side also in addition to privacy.

Mr. Charbo: You know, you take that a topic at a time. So at least I do, so you look at a subject area and we can take a situation at hand and say, situational awareness, as we move into the next disaster season. So the integrity that we look at in terms of that data is, are we seeing as current or as accurate a picture as we need to or as we want to at that time? And as you begin to distribute that data, are we maintaining the integrity of that data as we distribute it out? Much of these are many time instances of the same piece of data. Here's an image at 10:00 o'clock. Here's an image at 11:00 o'clock. Here's an image at 9:00 o'clock. Without those MEDA data tags of 9:00, 10:00, or 11:00 I may assume I'm looking at the same image unless I really look at details and see that it's changed. So a lot of the issues that we look at in terms of the integrity revolves around how we place those MEDA data tags to assure or provide a greater integrity or visibility into what piece of data are we actually looking at. A lot of that comes from the owner, you know, the owner of the system or the owner of the data since it's their business process. You know, they need to be assured that they're also looking at -- and we do rely on them to provide whether or not the integrity of that data set is what they state or what it is. But I tend to look at it in terms of a topic at hand rather than here's an integrity magic bullet and it will solve the whole problem.

Mr. Barquin: I don't -- I guess I don't want to suggest that there is such a thing as an integrity magic bullet but I do believe that there are some useful programmatic activities on the integrity side that maybe at some point -- I know the office, the privacy and integrity office should suggest and that we should look at more carefully in the future.

Ms. Sotto: Thank you, Mr. Barquin. And thank you very much, Mr. Charbo, for your comments. Our next speaker is Luke McCormack. Mr. McCormack is the U.S. Immigration and Customs Enforcement Chief Information Officer. Mr. McCormack has also served as Acting Executive Director of the Infrastructure Services Division of the Office of Information Technology at Customs and Border Protection. Thank you for joining us.

Mr. McCormack: Well, thank you. Much like Mr. Charbo I just recently joined on to Immigration and Customs Enforcement. My first day was July 25th. And I've been working with the CIO community prior to that and certainly now under Mr. Charbo's leadership and I must say that we've been making a lot of progress. I wanted to do a couple of different things just to kind of give you from a CIO, component CIO's perspective, some of these things that are underway and talk about some of the things that we think about while we're building these systems. First of all, from a privacy impact assessment perspective in the remediation process, my security manager for example also has -- well actually has two performance elements. One is a 100 percent assessment of all of our systems based on the FISMA assessment. And, two, along the lines of what you folks were sort of touching on is not only analyzing the systems that are out there today but baking in a process so that when we build a system we incorporate the privacy impact assessment into the building of that system. And that's done through the STLC, the system life cycle management, through gate reviews where we're assessing these systems as we're building them. And that way we do have awareness as we build these systems, post the investment process, if you will. Scott mentioned I am the subcommittee chair for case management at the department and what we're doing there is we're taking a look through a sort of a portfolio management view of all the case management activity that's going on in the department and looking at exploring opportunities there for alignment, certainly looking at opportunities where when we start to align these investment, these systems, where we can align the services as well. And that would include services where we can ensure that we have non-repudiation when we're accessing these systems, how we're sharing the data when we do share it. A lot of this is focused on standards right now and the different types of nomenclature that we're going to use on these standards. This is not only within the department, this is with the Department of Justice, this is lining up to the OMB line of business as far as case management is concerned, and the data associated to case management systems. It's certainly based on an architecture. We want to make sure that when we're building these things we're all building it the same way or in a lot of cases if it's service we're building it once and using it many times. When we build a system internally within the component we're looking at trying to, where the system's going to be sharing data, we have standard MOU's in place, we have information security agreements in place, we're going to do a privacy impact statement as we talked about. We also concern ourselves with things like third party rule and system of record. Those things are very important and we need to make sure that we maintain those and that we build some type of security structure around that so that we can maintain the integrity of the data. One other things that we wanted to point out, ICE just happens to be sort of the, I'll call it the legacy steward of the PKI environment that was built for the departments now being leveraged. We're looking at taking some of these capabilities with TWICs and some of these other identity management type capabilities and fusing them together and offering that as a service for the department. Once again, this is build once and use many so, questions.

Ms. Sotto: Thank you very much. Questions. You left everyone speechless. Okay. Our next speaker is Frank DiFalco. Mr. DiFalco joined the Department of Homeland Security in May of 2004, and serves as the Deputy Director of the Homeland Security Operation Center. Prior to coming to DHS, he worked for Anteon Corporation at the Office of Naval Research where he was responsible for strategic plans and operations for a futuristic command center program. Mr. DiFalco retired after 26 years in the U. S Marine Corp where he earned numerous honors such as the Legion of Merit Medal and the Bronze Star Medal with combat V. Thank you for joining us, Mr. DiFalco.

Mr. DiFalco: Thank you and good afternoon. What I was going to do was talk a minute about the Homeland Security Operation Center for those of you who are not familiar with it and then also touch on the Homeland Security Information Network because both of those together really play into the privacy impact and other issues. The HSOC is a standing 24/7 multi-agency organization and what we do there is we collect, fuse, and share all source information at all the classification levels. So it's kind of a hybrid. It's one of the few places that fuses intelligence as well as operational information. The mission of the HSOC is that the HSOC serves as the primary national level hub for daily domestic situation awareness, common operating picture, information fusion, information sharing, communications and operations coordination pertaining to the prevention of terrorist attacks and domestic incident management. The easiest way to think of it is if you think of the HSOC as the ingestion machine for DHS. All source information coming in, it comes into the HSOC and I mean information, raw data, not information that's been turned into intelligence yet. So we're talking raw data, unvetted information. It comes in, we collect it there, we do a -- basically we have a 24-hour cycle.

We do a quick look at it, see if there's any terrorist nexus, kind of the indications and warning arm for DHS, and then we pass that information or that information goes to IA, information analysis. And there they do a deeper dive on it for trend analysis and other activities to put the pieces of the puzzle together. And then those pieces go on to infrastructure protection which can include state and local, private sector, and anyone else that needs the information. The key is to make the information actionable, to make it operational. Otherwise, you have information and you don't give it to the right people, what's the use of having it. And that's what we do there. The main thing is looking for a terrorist nexus and the process I just described I know it seems linear but it's not linear. Information analysis, infrastructure protection, they're all imbedded, integrated into the HSOC. So as the information comes into the HSOC, IA is looking at it right there. It's their people in there looking at it from an intelligence standpoint. Infrastructure protection is looking at it at the same time from an infrastructure standpoint and there's over 40 agencies in the HSOC, federal agencies, national intelligence agencies, law enforcement agencies, New York State Police, LAPD, Boston Metro P.D., FPS, all the different agencies, ICBP, all the border agencies, Coast Guard, everyone's in there, all the emergency management agencies are in there. This gives us the capability to quickly get information, de-conflict it or verify it, and then take action on it with what we want to do with how we're going to share it and also vet it for sharing. On a daily basis, the HSOC collects operational and terrorist related information from all available sources across the United States. We maintain and share daily domestic situation awareness. The key word is domestic and we act as the indication and warning element for DHS. Incident management is our other role. The NRP designates us as a national level hub for domestic management and operational communication and information sharing for any type of catastrophic event in the United States so we're the primary conduit to the Secretary, his leadership team and to the White House Situation Room for catastrophic events. The Homeland Security Information Network is the primary DHS conduit through which information on domestic terrorist threats, suspicious activity and incident management are shared at all levels of government to include the public, private sectors. Okay. HSIN, what's called Homeland Security Information Network, is a network of networks with the internet and data sources that support multi communities of interest. It's a friendly user system that provides an array of capabilities at no cost to the end user. So this rolled out at no cost to state and local, private sector or anybody else that needs it. It enables federal, state, tribal, local, territorial and other organizations to include international and private users to be able to communicate and share information with each other in a real-time, secure environment and it's encrypted, the 128, the 192 bit encryption; and the system provides direct access to an extensive suite of functions that include mapping, search engine, instant messaging and collaboration chatting and information posting capabilities. It interfaces with the Department of Justice LEO systems and RISK system. The communities of interest, it's divided into communities of interest because each community has its own rules, like we talked about earlier. Like law enforcement has different rules for people that can see it, groups that can see it. The private sector has their own, there's intelligence, everyone's got different categories so it includes law enforcement, the critical sectors, the ISACs. It includes the critical infrastructure which is now called P-3, public/private partnership, which is the private sector. There's a secret level portal in there that went out to all the states and several of the major metropolitan areas. It has an international portal on there that includes Canada, Britain, and Australia, and there's an emergency management portal. The HSIN is rolled out, it's operational in all 50 states, the District of Columbia, five U.S. territories, and 53 major urban areas. It's operational in the three foreign countries that I mentioned and there's about 50,000 members of various communities of interest. Forty thousand of them are in the private sector right now. We expect that to go up into the hundreds of thousands by 2007. And the secret portal is operational in all 50 states in their EOCs, emergency operation centers and 18 additional law enforcement agencies. One of the key parts for information is situation awareness. Eighty percent of situation awareness is a common operating picture and for DHS the common operating picture is a map of the United States with the infrastructure of the United States imbedded in it with an overlay of suspicious activity and with blue force, friendly force, overlay on that. So at any time you can bring up anywhere in the country what the infrastructure is, what the suspicious activity is that's going on around it, and what blue forces, what friendly forces are available to effect that particular suspicious activity or event that's going on. And it's also used in incidents, incident management like for hurricanes and stuff like that. But that gives us the picture to be able to make better decisions, better situation awareness for decision-making. Now, information sharing is important to the Homeland Security Operation Center because it increases the national unified effort, an increase in situation awareness to make better decisions, and it increases execution effectiveness overall at all levels, strategic, operational, and tactical. The information sharing environment is beneficial to everybody, it's necessary to win a war on terror, and it's subset of a command and control issue overall for the nation. The primary obstacles I believe as mentioned earlier, I think Scott mentioned that they're not technological, they're cultural, and agencies, inter-agencies, whether it's intra inside DHS or with other agencies we deal with, everybody's used to doing their own, kind of doing their own thing, reporting to themselves or not having a unified effort. So there's a tendency at times not to share information or not to share it fast enough. Speed of information's a big deal. In the information age, slow information is as good as no information. And a lot of the obstacles just end up being things like rice bowl issues with agencies, you know, they kind of play the one-upmanship game at times with what, you know, they know and you don't know and that type of thing. And there's also some technical part of it because agencies have closed networks. Some of them they'll have their own networks that no one else is on and they don't want anyone else on them. We have those in the HSOC. They'll come into a desk officer there and that desk officer's on it and can pass the information but it is not interactive. It's not interconnected or it's not integrated into the other networks that are in the HSOC. And privacy throughout this, we deal with it all the time, especially taking all source information from all different agencies with all their different rules and then trying to fuse it and share it at all the classification levels. So it's a use issue to us and we have people on several working groups trying to work through these different issues. Okay. Thank you.

Ms. Sotto: Thank you very much, Mr. DiFalco.

Ms. Lemmey.

Ms. Lemmey: I got to go visit at least one of the facilities during the top off exercise which has hopefully changed because there was a lot of folks crammed into a little space. But it was an interesting discussion because obviously you guys are getting -- or as it was described to us at the time, you're getting a lot of information from all over, anywhere, all kinds of people calling with all kinds of stuff much of which is junk that you're sifting through. And, it seems interesting at the time that a lot of that is U.S. persons data which has no relevance to known or suspected terrorists. And yet there are so many other organizations residing with you. How -- I know you were talking about having some walls and some barriers, how are you guys handling that from a privacy perspective with so much information getting tossed over the transom at you and what's your sort of plan with going forward with that?

Mr. DiFalco: As that information comes in through the particular agency or whatever the venue is that we get it, the desk officer there looks at it, helps us sort it for okay here's information in here that's a privacy issue or that's another type of issue whether it's a classification issue or whatever. And, then within the HSOC that gets passed around because it's -- we're federal and intel as well as law enforcement, you know, because of the law. And so we're able to take a look at it. Before sharing that or pushing that information out, it gets vetted, it gets looked at. There's several -- like an example is the Homeland Security Information Bulletin goes out every morning. That's done in a group collaboration effort where they put it up and we go through it, they go through it and make sure there's no law enforcement sensitive information that -- there's no specific name of a company. You know, that we don't say, you know, company A we say, you know, a department store. We try to make sure that it's vetted enough that we're not putting out incorrect information or violating any of the laws. We also try to make sure that we go back to the agency that provided the information and let them know what we're doing with it, if they don't already know when they send it in. Sometimes they'll send it in and say you can disseminate widely or they'll have instructions on it. But we go back to the originator when we have to make sure that they know what we're doing with the information.

Ms. Lemmey: Just as a quick follow-on, one of the comments that we heard this morning is about information going in and not coming out or never being able to be removed. Since you guys get a lot of stuff that turns out to be not very relevant, whether it's people calling in about their neighbors or something else, what is the process for removing a lot of that data that's not relevant about U.S. persons?

Mr. DiFalco: I don't -- that process is not actually in place. I mean, there's not a real good process for that. That's part of the working groups trying to work through, okay, when you get it in how long do you keep it? How do you know that it's not relevant -- might not be relevant now, how you know it's going to be relevant in the future? That's all getting worked through. It's a concern and those are issues that we deal with that we're trying to work out.

Ms. Sotto: Thank you. Mr. Hoffman.

MR. Hoffman: Director DiFalco, thank you for being here. Two questions, first, do you keep an inventory in some respect of the data sources and where all the different streams of data that are coming into the HSOC are?

Mr. DiFalco: Well, we keep a -- we have the agencies and their networks.

Mr. Hoffman: Yeah, so I guess the question I, the better question I should be asking is, is the streams of data coming into the HSOC just the agencies or are you separately going out and looking for other data to supplement that with, for example, contracting with commercial data?

Mr. DiFalco: Well, the commercial source of that data comes in through the infrastructure protection desk which is the National Infrastructure Coordinating Center, has a desk officer in there all the time so we get information in from them. We get information through the critical sectors. There's parts of IA that do open source information, searching, we get that. So it's all coming through the desk officers to include the media, information that we get in. But there's not -- we don't go out on separate searches for information. Our streams come through the agencies that are in there.

Mr. Hoffman: So these are agencies that are separately collecting this data for their own purposes and you are a place where that information is being consolidated and analyzed, a certain subset of.....

Mr. DiFalco: Yeah, and they do their own collection, their own analysis for what they need and they pass stuff on.

Mr. Hoffman: Okay. That's helpful.

Mr. DiFalco: Yes.

Ms. Sotto: Thank you. Mr. Purcell.

Mr. Purcell: Thank you, Director DiFalco. With all of this information there, could you clarify for the committee what the status is of the PIA or multitude of PIAs you must be working on constantly? It sounds like a ton of information and there must be a multitude of systems. You also inherit PIAs because not all the systems are, I mean, they're not all directly under your control but there must be some I would think.

Mr. DiFalco: The agency systems are under the agency control but they terminate in at the desk officer in the HSOC and we go with their rules. Some of them are working privacy act issues or the PIAs. We're trying to work them out. It's a huge effort. There's several working groups who are involved in all of them for DHS and with information analysis, the privacy act office for DHS, and we have, you know, legal officers as well as operators that are on those groups trying to work this out. It's a -- all this is kind of like your expression's been used that you're building the plane while you're flying it because the, you know, activities are ongoing and suspicious activities happening and it doesn't stop to work out a process or a network or that type of stuff so we're running at the same time trying to make sure that we're complying with all the regulations. And there's lots of gray areas as you know between intelligence and law enforcement and those type of things and privacy act issues. So the PIAs are being worked on. They're not definitive yet especially for all the different networks that we have in there.

Ms. Sotto: Thank you. Sam Wright.

Mr. Wright: I have a question for Mr. Williams, if that's appropriate.

Ms. Sotto: Please.

Mr. Wright: That U.S. VISIT Program is -- deals both with visitors coming in the country and then exiting the country, and I know that the exit process if through the kiosk and what have you is largely a voluntary process at this point but I think the level of comfort that our foreign visitors have in the entire process and the way records are maintained and the privacy aspects of that, you know, there may be some reflection in that comfort level with the level of voluntary compliance as they leave. I was just wondering if you had any comments or observations on just what that level of voluntary compliance is on folks exiting the country.

Mr. Williams: Sure, I'd be glad to. First of all, when we're talking about exit, let me separate exit between people leaving through an airport or a seaport versus leaving the land border. Land border's a tough challenge but so is an airport or a seaport. And let me just describe the environment we have today. We have all the infrastructure and facilities we need for people entering the country but different from a lot of other countries, if a foreign visitor leaves Japan through Narita Airport, Poland, Israel, even Mexico, other countries, think about going out of Narita Airport in Japan, when you leave that country to go on an outbound flight, you go through immigration control, you go through a passport stamping place, you go into a secure part of the airport. You are effectively checked out of the country. If you want to come back in, you have to check back into the country. Contrast that with leaving through Dulles Airport. You go to the international ticketing counter or ticketing booth, ATM or kiosk, you go through TSA checkpoint, you go to the gate. There's nobody from an immigration standpoint who checks you out of the country. What we're trying to pilot-test right now through the use of kiosk and mobile devices in 12 airports and two seaports is biometrically collecting that information, again, trying to meet our goals of making sure we can know who's leaving the country biometrically, doing it in a way that protects their privacy, but also doing it in a way that does not adversely impact legitimate travel. And the airlines are very concerned about, do we disrupt the boarding process? And we've been pilot-testing this and we're making recommendations how to we go forward with exit to airports and seaports. It's not easy because the United States -- we don't have that permanent infrastructure to deal with but we are trying to make sure we can meet the requirements of the law, and it is a law that we implement biometric exit. We do believe that there is great benefit in doing the exit and in fact the pilot tests that we have right now are not voluntary. Where it is in those 14 airports or seaports, it is mandatory. Our compliance rates have not been great, however, we had a recent turn of events where ICE deciding to do an outbound operation at a particular airport where they looked at their airport as a hub for illegal alien smuggling, pulled people off of planes, did biometric checks on them, and found out many of the people had not checked out as they were supposed to. What happened in that airport was our compliance rates were maybe around 30 percent. They shot up. And all the airlines because they were and airports who were concerned that we would disrupt their boarding process, wanted to help us comply. And I've compared this climate to the Indiana Jones movie where he's on the airship and he's posing as a ticket character and asked everybody for their tickets and the German guy doesn't have one so he throws them off the airship and everybody holds up their ticket, they want to comply. And we believe, however we're going to do exit, it's got to have enforcement behind in and there's got to be consequences if people don't comply. And if we make it nationwide in some form, it will increase compliance. And, again, all we're trying to do is be able to biometrically verify that somebody has left the country. We think there's -- it's the law to do that but there's also great value to do that. How we do that, we're still debating, and we want to meld it into the traveler's experience as much as possible. Some day you may do it at the ticket counter and some day you may walk into an airport and this is your credit card and this is your boarding pass and this is how you check out of the country.

Mr. Wright: Thank you.

Ms. Sotto: Thank you. Mr. Hoffman.

Mr. Hoffman: Director DiFalco, following up

Mr. Purcell's question, you mentioned that there were several working groups looking at questions on PIAs and you're resolving some issues and talking back and forth and that sort of thing. Could you expand that just a little bit? Is there a formal structure to these and is there -- are there any -- is there any documentation or record on when they meet, what conclusions they come up to, they come to, and how long has this been going on and how does this work? Can you expand that a little bit?

Mr. DiFalco: Yeah, there's a -- the working groups, there's two or three different ones that are at different levels within HSOC, within and including IA and NALTA to resource some of the other directorates as it's been reorganized and they have the meetings, they go through the processes, they identify -- there's draft papers that come out on, you know, these are the drafts on what we think the rules are going to be for this. It's under legal advise -- you know, it goes into the lawyers of DHS to kind of have final say on whether it's correct or not and up through the privacy office. But I'm aware of any that -- I think the question I was asked is there one in place for it, you know, that kind of fixes it and I'm not aware of one that actually nails down all the requirements for us yet. But there is -- it's written, there's information on it, there's draft papers.

Mr. Hoffman: And the privacy office gets those?

MR. DiFalco: Well, I assume they do, yes. I would have to check that specifically.

Mr. Hoffman: Okay.

Ms. Sotto: If you could follow up on that, we would be grateful.

Mr. DiFalco: Okay.

Ms. Sotto: Thank you. Mr. Barquin.

Mr. Barquin: This question is for Director Williams. I know that right after U.S. VISIT was deployed, there was at least one country, if I remember correctly I think it was Brazil that said okay you do it to us we'll do it to you. And I guess, first is, have there been other such situations in general now that U.S. VISIT has been out there for a while, has that died down? The second related question is, what are the metrics -- I mean, you mentioned 51 million people having been put through U.S. VISIT, but in general do you get a lot of complaints? Is it a fairly unintrusive and fairly quick process and what kind of redress mechanisms do you have?

Mr. Williams: Thank you for the question. First, in terms of the question about what other countries have done, right after we implemented, just so people know the history, in Brazil there was a rogue judge who, exceeding his authority, decided to retaliate and decided to 10 ink print Americans and frankly take pictures with Polaroid photographs and hold them for many hours. We expressed our disappointment at that reaction because it was a knee jerk retaliation action. What's happened since then is just the opposite. Other countries are starting to adopt exactly what we have done here at the Department of Homeland Security and in the United States. As Secretary Ridge said to us before he left, he said you all have changed the world. Japan is starting what they call Japan VISIT, what they say is modeled about U.S. VISIT. The UK in their e-borders program, the EU in their visitor information system. What I've been talking about is taking 10 prints on enrollment for people who want a visa to come in the country, you can see that today at the Belgium Embassy here in D. C. You can see it at the French Embassy in San Francisco. You can see it Thailand. They're doing exactly what we're doing today. And that's exactly what we have encouraged, is encourage other countries to lift up their immigration border management system. We're not alone in trying to stop bad guys, people who by any definition would be a terrorist, and trying to appropriately share that information and trying to make sure that if there are bad guy fingerprints out there of terrorists, we want them. And I would suppose Australia wants them, the UK wants them, France wants them, everybody wants them. What we're trying to do is work in accordance with international standards to lift up, to at the same time stop bad people when they try to surface and travel and do harm. But also to help good people travel. Make it easier for good people to travel. So we've seen after that that one instance of that rogue judge, who by the way was quickly overruled because it was perceived that he was going to disrupt the flow of Americans wanting to come to Carnival and that was taken very seriously. So that was stopped rather quickly. People didn't want to have American tourists stay away for that reason. And tourism is huge. In this country it's a multi-trillion dollar industry. It's been estimated one out every eight non-defense civilian U.S. jobs are tied to travel and tourism. We want to make it easier for good people to travel and frankly across the globe. That's what we're trying to do. And, you know, we're working closely on just a biometric passport testing with Australia, New Zealand, and Singapore right now. That's what we're working together on in San Francisco Airport. So we want to strengthen and improve immigration border management systems across the world. In terms of metrics how we measure ourself -- well, first of all, I told you we've processed 51 million people. In terms of our complaints and redress, we have a U.S. VISIT privacy officer by the name of Steve Yonkers, works very closely with Maureen's office and to date we've received out of 51 million people processed about a 140 requests for redress. And I'll tell you what most of those requests are. It's where a husband and wife came together and they think their fingerprints were mixed up and in some cases they've actually been right where when their finger scans were recorded it was the husband's associated with the wife's and then they've got -- they were stopped the next time around because it didn't look like it matched. And we fixed those very, very quickly. That's been the majority of the complaints we've had is things like that. In terms of other metrics, measuring whether we've had an adversely impacting commerce, in our airports we've actually slightly decreased the processing time. And part of it is you've never seen U.S. VISIT -- if you go to Dulles Airport and go to the foreign visitor line when somebody puts down a digital finger scan and I'll give a lot of credit to our CIO people, what you see is about five to 10 seconds after that person has pressed send on the prints that screen of the officer, his or her screen, is blinking red or green. If it's blinking green they know it's not a hit. And if we had those fingerprints previously they are who they say they are. That gives that officer, gives his or her, a feeling about that person more confidence. They still do the interview. If it's red they immediately take the person out of line thereby speeding it up for the rest of the people. Actually at the land borders where there was great concern, we even had demonstrations on the southwest border against U.S. VISIT, everybody was afraid we were building fortress America, and we said our goal is exactly opposite. We believe we can enhance security and facilitate legitimate trade and travel at the same time. The land borders we've actually speeded up the processing of people because we added other improvements such as printing out a pre-populated I95 form. We took in Laredo, Texas, where it was taking 10 to 12 minutes per person down to two to three minutes. And if you talk to the port director in Negales, James Tong, and I love his quote, he said it right in front of me, he said, U.S. VISIT saved our bacon. During the holidays when they had people backed out the door trying to come in the United States as they do from Mexico, people often get discouraged and just turn around and go back. Because of U.S. VISIT he was able to speed up the process while enhancing security at the same time. So we've, in terms of our goals, we've only had a 140 requests for redress out of 51 million. We speeded up the processing of people. In terms of security, I mentioned the State Department using our system over 15,000 I think it's now 16,000 biometric hits. For us we count only those people we take adverse action against, not all of our hits. We stopped over 1050 murderers, rapists, child predators, drug traffickers, and serious immigration violators. Now, let me tell you one more story about how this system works. True story. DOD captures a guy, takes his prints, he escapes. DOD sends the prints to the FBI. FBI sends them to us. This guy makes his way to Amman, Jordan, applies for a U.S. visa, puts his finger scan down, immediately it's a hit. It's this guy who was suspected of terrorist activities who escaped from Iraq. Interpol gives us prints and the first print they gave us we -- they gave us a few sets of prints. They wanted to see what it was like. We take all the people who are in our enrolled database, unique people we process, it's about 39 million right now. Every time we get a bad guy update which is every day we run it against a good guy because good guys often become bad guys. Interpol gave us a small amount of prints. We immediately get a hit. It's a guy who is Bulgarian who moved to Costa Rica, became a Costa Rican citizen, applied for a U.S. visa, got that but had not yet come. We then found out by running his -- he's in the good guy database -- against the Interpol prints and said this guy's wanted for embezzling nine million euros, Interpol's been looking for him for 10 years. He's called in on a pretense in Costa Rica and they arrest him. Interpol says this is great. They give us more. The next guy we hit against is coming across with an alias. He's a commercial truck driver, coming from Canada regularly through Lewiston, New York. He's wanted for murder and attempted murder out of Germany. He's a Republic of Georgia citizen. And sharing that information about people that 1050 is something we're very proud of when we can stop those murderers, rapists, child predators and drug traffickers. One drug trafficker we knew had come into the country 60 times in the last four years. He was in various aliases, as he's from Jamaica said I was just doing stuff. That was his -- what he was doing. But I mean these are people -- I'm sorry -- but these are people hurting our children and it feels good for us to stop them. That's part of how we measure ourself. And part of it is, you know, people say we only ever catch the dumb terrorist. Well, we catch a lot of dumb people but, you know, frankly 9/11 is alive in our office every day. We don't want to have those people get through. You know, as soon as prints are picked up from a London bomb site, you know, July 7th of last year, those prints come to us as latent prints. We then run them against the 39 million to say have we ever seen that person before. And the same thing we're doing right now with prints we're getting from DOD from various theaters where they collect them. We do measure a lot of different things.

MS. Sotto: Thank you. Mr. Hoffman.

Mr. Hoffman: Director Williams, I want to address a couple of your comments and then ask some questions. You talked earlier about enforcement and I'm hoping we pause for a while before starting to throw Germans out of planes because having known a number of Germans who've been going through U.S. VISIT, I can tell you there's a huge misunderstanding about what people are supposed to do when they're going there. I think we could strive quite a bit at what our disclosure is and what -- and maybe this is getting better, but my experience is watching people go through it. There's a lot of people who don't even understand what they're supposed to be doing. There's a lot of people flying who don't even speak English and have great difficulty understanding. So you mentioned earlier that you have provided notice about the collection of the information and the uses of the information and you've described three or four different purposes I think for the use of the information, matching the information at arrival and exit, use to be able provide information to law enforcement when they need use to be able to catch a terrorist. Just wondering if an individual wants to understand how their information is going to be used, how do they get access to that. I know there's a systems of records notice but when I fly I don't see anything where there's a privacy policy or something that's handed to people letting them know how their information is going to be used and I'm wondering if there's some work we can do there to better communicate to people so they've got confidence in our government.

Mr. Williams: Well, that's a good question,

Mr. Hoffman, and what we know is you can never communicate enough and that's why we spend a lot of time frankly trying to make people aware of what we're doing around the world. I will tell you my deputy spends a lot of time on the European continent. I was just in Frankfort maybe about three months ago talking to people about what we're doing. We want people to know, not only through publishing in the federal register, but we know that we have to conduct outreach and we do that wherever we can. And I always give people the same offer when I meet with people who represent constituent groups, tell us where we can stand with you and communicate about what U.S. VISIT is and try and answer their questions about what information we're collecting, what we're doing with it. We try to be out there talking to people as much as possible. We talk to the Germans quite frequently, the German government, and when I've been over there and my deputy's been over there and others, we set up meetings where we can talk to like the travel industries and people who are those force multipliers for a communications that can help us get that message out. We also try to put signage in all of the airports and seaports and land borders so that people can see the process in any language. And if you go to Dulles Airport you'll see our signs are in multiple languages. And we try to also customize that to where people are in Chicago you'll see Polish. In the west coast you'll see Japanese and Korean often, yeah, trying to make sure at least people know what to do to comply right there. We don't go into great detail about what it is we do with the information but you can see that through our website that we give out to everybody. We also offer to put people on a list serve that we have where anybody wants information, you know, where they can get blast emails from us and we promise never to let them off that list. We do that so that people can constantly get updated about what we're doing. If you have other suggestions for how we can communicate what we do with that information, I'd be glad to listen.

Mr. Hoffman: Yeah, I think if you would be willing to, I think we might have some followup questions that we could give to you and specifically maybe provide some help and some guidance on how to provide privacy notices that comply with sort of the standard methods that are used to provide information to people about how their information is processed and collected. That would be okay?

Mr. Williams: We'd be glad to do that. I think in some sense what we did is becoming a little bit of older news where we also surveyed travelers one of our metrics and what we found was people saying it's no big deal, for the people who have been through it. Now maybe they do have more concerns about their information, what we're doing with it but as we survey travelers, they really said this is no big deal. I always tell people to go see it. It's underwhelming when you actually see the process. But I know there's concerns about the information and we'd be glad to listen.

Ms. Sotto: Thank you very much to this panel. This was a great panel and we very much appreciate your joining us. To the extent that we've asked for followup information, Becky will be contacting you to make sure that we get our questions answered and we are deeply appreciative of the fact that you took time out of your busy days to be here with us. Thank you. I'd like to remind members of the public that if you'd like to sign up for questions you can do so outside at the desk. See Lane Raffray. He's outside and he would be glad to take your name down for questions in the public comment period. I'd like to now turn to our subcommittees to make reports so I would ask the chairs of the various subcommittees to be prepared to comment on the status of their subcommittees. I'd like to start with Charles Palmer. He needs to leave a little bit early so Charles is the chair of the emerging applications and technology subcommittee. Charles. SUBCOMMITTEE REPORTS, REPORT EMERGING APPLICATIONS AND TECHNOLOGY SUBCOMMITTEE

Mr. Palmer: Thank you, Lisa. I have to say this particular meeting was one the more enlightening meetings, primarily because of the guests that the staff was able to arrange to come visit us. We're exploring automatic identification technologies, RFID in particular. We may proceed on to others after that but RFID seemed to be the one of most interest at the moment. And, of course, we're only exploring those applications of RFID that have anything relating to tracking people. We're not addressing tracking material other than in the possible combination or secondary effect of tracking material tied to people that would allow you to tie the tracking to the people after all. So we met twice during the interim since the last meeting. Working on drafting a white paper summarizing our recommendations and we are aiming for a short readable effective white paper, not a tutorial. There's plenty of those around. In particular of value this past Monday or yesterday we discussed and refined our draft and set our time-line for completion and submission to the full committee for their comments in June. That's a very aggressive time schedule given the fact that yesterday we also met with several members of DHS who are involved in the RFID, various RFID efforts in and around DHS. We were I think pleasantly surprised at how much work they had done, how much thinking they had already done about privacy and the concerns and we are expecting to receive a few documents back from them to use as input to our final paper. Let's see. And we certainly appreciate the time that they spent with us which was far more than was scheduled and there were far more of them than we ever expected. I think we had about nine people anxiously come join us to explain what they were doing and answer our questions so it was extremely productive. We expect to have two more subcommittee meetings in the very near future to try to make sure that we accelerate and get this thing done because as the emerging applications and technology team there is a whole list of things that people are asking us to look at and provide advice and commentary on so we need to get moving. With that, thank you.

Ms. Sotto: Thank you very much, Mr. Palmer, and thank you to the members of the emerging applications and technology subcommittee. I'd like to turn next to the framework subcommittee. Joanne McNabb and Jim Harper co-chair that subcommittee and first I'd like to thank them very much for their patience and their perseverance in creating a very important document, the framework document, which they're going to be presenting today for adoption to the committee. Joanne and Jim. SUBCOMMITTEE REPORTS, FRAMEWORK SUBCOMMITTEE.

Mr. Harper: Thank you, Lisa. Members of the committee I think are all very well aware of the document and what it looks like for the few people attending late this afternoon apparently there are copies of it available, the proposed -- the version proposed for adoption but I'll just briefly run through it. It's a recommended framework for analyzing programs, technologies, and applications. Being recommended makes it far from mandatory for our use but maybe a helpful issue-spotting document and an outline for possible use by subcommittees as they put their documents together. It's a five-step document starting with the I think essential topic of scope. We should know what the subject of the matter is. Where appropriate, legal basis, that is the legal foundation for a particular program or use of technology and so on and so forth plus perhaps legal limitations on a program or technology, all as relevant. Particularly with reference to witnesses that we heard from in Bellingham, I think Joanne and I and the subcommittee and many members of the committee recognized that it's important for programs and technologies to have a coherent story about what they do, about how they make the national security efforts go better, how we're better off having the programs in place. And so we spent a lot of time studying risk management. It seems quite far afield from privacy when you first come to it but it seems after spending some time with it it's actually essential to be able to say what a program does, why we're better off with it, because then you can judge if some diminution to a privacy interest is worthwhile in light of the program's results, it's efficacy. So step three walks through one type of -- one approach to risk management. It's not the only way to express the benefits that you can get from a program or technology, but again it's a recommendation or one way of hopefully helpful way of thinking about these problems. Step four is the hear of the matter for us obviously which is to look at the privacy interests affected by a technology or program. And we've done something that's different I think but fairly well rooted in traditional privacy analysis. What we've done is try to take some of the fair information principles and turn them inside-out or turn them around somewhat so that we leave with the values. As a person who communicates to the public a great deal, I'm aware for myself that a lot of people are indifferent or unaware of the FIPS. We all, all of us, work with them constantly. But I think we can do more forceful work ourselves and the privacy office and other DHS components can do better work by understanding that there are real meat and potatoes American values behind privacy and that a lot of the actions and processes and functions that we ask of agencies and we've asked of them today to tell us about reflect things that are very important to all Americans. Finally, step five of the paper is a recommendation sections relatively open-ended. Anybody can do with it anything they want. It's obviously at the tail end of a paper, you should have something to say about the program, so we recommend doing that. Again, a framework, I've worked with it some to try to take our RFID work and framework it over and it's challenging. It's frankly quite -- it's quite hard to do but I think that's because a lot of this thinking isn't being done or isn't being done clearly enough or made available enough to the public. So we have a lot of work to do ourselves to reconcile the things we're working on with clarity, with good public discussion about these things. So I think Joanne is going to talk some about process and some changes that have happened to the document as we worked through the committee.

Ms. McNabb: Thanks. An earlier version of this has been -- a couple of earlier versions have been posted on the committee website since September when it was since after the September meeting and I wanted to highlight the changes that have been made in this most -- since the last meeting in December in particular, that the structure of going through the steps is the same and there have been a number of changes made in response to comments from the general public and from other members of this committee and of the subcommittee. So just a couple of the more recent ones I wanted to point to. In step three on page three of the document in the second paragraph, it was more clearly emphasized that what is being asked for in this step is a statement of what are the benefits of the program, what is it going to do to protect homeland security. On page four in step four, throughout step four, we pointed to with these little subtitles in all caps, we pointed to where the fair information practice principles are represented. The original approach and still the basic approach is to look at the underlying values that are components of privacy and related to privacy. But then those guidelines that are not only used in the U.S. in many places but also in other parts of the world where they pay attention to information privacy, many of them are involved in this analysis and we've given them their title so you can find them easily. And, finally, oh one more, we added on page six, we added an accountability item which hadn't been there before and that is one of the fair information practice principles. And then the some of the clarifications and definitions and explanations in the footnotes have been modified here and there and we do have -- we have a manager's amendment, Jim says it's called, in the California's legislature we'd call it a author's amendment, but anyway to propose but Jim is going to propose.

MR. Harper: Let's call the whole thing off. No. [Laughter]. We did receive a great deal of helpful commentary that continued well into yesterday and one of the very improving suggestions that came up was to modify on page five the bullet titled freedom from surveillance and take that sort of difficult locution and use the best most accurate word for the interest represented by that and that we came upon as seclusion. Seclusion is one of the four, is what's protected by one of the four privacy torts that are well-known in American law and I think it's valuable to express that interest with the most accurate language, which is calling it seclusion. Surveillance is a provocative term to some degree and we've had some good discussion about what is surveillance as opposed to more inert data collection and things like that? I think Joanne and I feel that the use of the term surveillance is appropriate in the discussion of that bullet and the trend we're all aware of with the expansion of data collection and the speed of data sharing is that data availance or ongoing surveillance of data is increasingly possible so it'll be helpful, it'll be startling to some but I think helpful for us and DHS components to realize that a lot of data collection goes to surveillance and so we think that seclusion is the genuine expression of the interest represented by that bullet. Continuation of the amendment is to have some more discussion of seclusion in footnote four on page eight dictionary definition, seclusion is the quality of being secluded from the presence or view of others, an important dimension of privacy that is eroded by surveillance. And as that footnote continues, the importance of it is this, that surveillance is not inherently wrong or harmful but awareness or even suspicion of surveillance in some contexts can inhibit individual sense of freedom, privacy, and self-determination. So I think we've represented well an important facet of privacy with this manager's or author's amendment. Should I move its adoption or what -- discussion?

Ms. Sotto: Is there -- I'd like some discussion or questions around this change. Joe.

Mr. Alhadeff: I wanted to be four for four. I've whined about every draft, why not this one? I actually -- I don't take issue with the legal concept of seclusion but I do take issue with the fact that I think we've tried to write this document not to be legalese and even with the definition that you give what you've seem to have protected is my right to hide but you haven't protected my right to be free from surveillance in plain sight and that really is what privacy is. So if we want to get rid of the word surveillance, I would suggest freedom from intrusion because that goes to the amendment that deals with this issue which is your right to be free from unreasonable intrusion. And so if we want to stay away from the word surveillance because I think surveillance is the mechanism as opposed to the concept then the concept for me is freedom from intrusion. Seclusion means, you know, I can become Howard Hughes in his later stages.

Mr. Harper: I think that freedom from intrusion remains a difficult legalistic locution and doesn't express as well the value. I agree that seclusion connotates to some extent hiding out, you know, in a darkened room but -- and I also agree that there are important issues around what remains private though you're presenting yourself in public but I tend to think that seclusion is the best term for what we're trying to describe there.

Ms. Sotto: Richard.

MR. Purcell: So I mean we're talking about Brandeis' right to be left alone concept I think more than anything else. Is that not right? Whether it's expressed as seclusion of the individual or freedom from intrusion by other individuals or whatever, I'm not sure it matters a lot but I just want to make sure to clarify for the record that is the concept of being left alone whether you're in a private or a public space, regardless of the space you're at.

Mr. Hoffman: To a degree the concept of being left alone is so broad that it actually kind of includes a lot of the different values we're talking about. The liberty bullet, for example, is the idea that I actually can act on the fact the information about me is not being collected, I feel the fullest range of opportunity to act. But, yes, essentially and one of the things I considered when we were talking through this is do we express this somehow as being let alone? But that's a little -- it's just, I find that an important hortatory but not a way of expressing exactly what the interest value is.

Ms. Sotto: Richard, this was my issue and I'll tell you what my problem with the word surveillance was. I didn't think that it adequately described what these three sub-bullets were. I think of surveillance as active surveilling of individuals as opposed to the more passive collection of data, if you will, a dossier on each individual so I was reacting to the term surveillance and Jim and Joanne were kind enough to try to think of another term that might better encompass these three sub-bullets or encompass them to the extent that I was having difficulty with the word surveillance. I'll tell you one thing that may have fallen out and maybe we can figure out how to deal with that, is surveillance of people. True surveillance, and I know I'm now contradicting myself, but I think we have two interests here. We have one active surveillance, a video camera, and then the second is putting together files, compiling files, dossiers of individuals and that's what you would call passive surveillance. I don't feel as though it rises to the level of surveillance in any form particularly because a file about an individual doesn't ever need to be really looked at so it doesn't feel like surveillance to me.

Ms. McNabb: But in fact the Department of Homeland Security, for example, compiles files in order to take actions. I mean, that's the purpose of gathering the data. I mean, and it's not just the Department of Homeland Security. I mean, I think it's very active surveillance to be gathering data on people, data other than the data of your picture. I don't see the difference between -- I don't quite see the active/passive distinction you're making.

Ms. Sotto: I think that we can probably cover both issues in the same paragraph and maybe it doesn't need to be revised but I just wanted to throw out my thought about the active -- I don't want to lose the active surveillance part. I don't want to lose the video camera.

Ms. McNabb: And that's data, too.

Ms. Sotto: It is data.

Ms. McNabb: Yeah.

Ms. Sotto: That's right. That's a good point.

Mr. Beales: I like the term seclusion. I like the -- and I think one of the strengths of the whole approach in this document is to look at the different kinds, the different dimensions of the privacy interest, and that this is a useful and valuable one. It lets us talk about some of the trade-offs among privacy values that Secretary Chertoff raised this morning that, you know, we certainly very much ran into in the screening subcommittee among the people who wanted to share terrorism information and, you know, were willing to subject themselves to strip searches and other people who would give up any amount of information in order to avoid the hassle of walking through the metal detector. And those are very real differences in people's values and in privacy values. I think sort of trying to break out the different pieces here which this approach does is a very useful way to try to do it.

Ms. Sotto: Ramon.

Mr. Barquin: I have applauded the work. I think it's extremely important. What I want to make sure is that we don't get bogged down again one more time with a word here and there because very specifically here we are in the screening subcommittee as I'm sure Howard's going to report later and we've sort of assigned to ourselves a task of actually reviewing a number of such programs and while this is out there in draft form it doesn't really have I think the mandate that it will once it's been approved. So I'd just like to suggest that we go ahead and then later on we continue discussion and, you know, come up with a better and improved version if necessary. But I think it's ready for prime-time. I'm going to use it anyway.

Ms. Sotto: I think we continue to have additional questions and comments. Are there additional comments on this particular point?

Mr. Wright: I'd like to say on this particular point that we should keep in mind I think some of the things Ramon was saying, if we look to the introduction that we have here as to the intended use of this document, it is a recommended framework not an absolute standard. And I think if we look at it in that vein I think the use of the word seclusion is perhaps as good a word as any but the objections to the use of the word seclusion in my mind do not rise to the level of let's put this on hold one more time while we try to find a different word. I would just note again in the concept that this is a recommended framework, I would just note that one of the bullets under seclusion is this use limitation which I think is a very appropriate statement of direction or guidance to be given to DHS and other agencies. And I say that in the context that we basically spent the afternoon meeting and hearing from folks who are in the information sharing business which to some extent cuts a little into the limitation of use bullet here. But, again, I think it's an admirable framework and I would move that we accept it.

Ms. Sotto: Just to be clear I don't think anybody has suggested not moving to accept this document today. We're just now talking about individual modifications. Is there another comment on this particular point?

Mr. Hoffman: This is not an individual modification because I just want to second very quickly Ramon and Sam, I don't think we should let the perfect be the enemy of the good here. And what has been presented to us by the subcommittee is about a thousand percent better than what is in place today. So I would second that if that was move I heard.

Ms. Sotto: You didn't hear it yet. One point that we've discussed internally that I'd like to actually make clear is that this is considered a living, breathing document. It is not a static document. We will revisit it from time to time. Processes change, notions and conceptions change, and this needs to change along with the sort of information environment. So I think we'll be making lots of changes to this document over time and in that vein I would ask for a motion to accept this particular amendment.

Mr. Harper: If I can, with thanks to Joe for always keeping it interesting, move the adoption of the amendment. Unidentified Voice: Seconded.

Ms. Sotto: Thank you. All in favor. [A chorus of ayes]

Ms. Sotto: Any opposed? [No response]

Ms. Sotto: Thank you. The adoption is amended. The amendment is adopted. [Laughter].

Ms. Sotto: Those A words. Jim, would you like to raise another point?

Mr. Harper: I think there's some other amendments that are somewhere between friendly and indifferent. [Laughter].

Mr. Beales: Jim, they're always friendly. I have -- I wanted to propose two amendments that I suppose, I'll present together and I don't know whether you want to do them as one or as two. If you start on page four of seven, I think one of the things that's really valuable about this whole framework document taken as a whole is it's a starting place to think about these issues, that is a much more sensible starting point. I think everybody has this. Does everyone have a copy? Okay. I think one of the things that's really valuable about the framework is it's a starting place to think about these issues that's a much more sensible starting place than the fair information practices by themselves. And toward that end I wanted to make this change on the last paragraph before the bullets on page four because I think this analysis really begins with the values that underline and inform the fair information practices, it doesn't really look to them and then however look at the values -- I mean, the starting place is really the values and I think, since I think to me that's a lot of the value of the document I think it ought to say it that way. The second change I wanted to propose is in the collection limitation and purpose specification, and that is.....

Mr. Hoffman: Howard, can I just ask can you articulate exactly what the first change was again? I missed it. The exact language.

Mr. Beales: Yeah, essentially it combines the two, the first two sentences that were there and it would read this analysis begins with the values that underlie and inform the fair information practice principles, or FIPS, the well-known set of guidelines for organizations on the handling of personal information. Okay.

Mr. Hoffman: I apologize.

Mr. Beales: The second change is on the collection limitation and purpose specification where the document as it is presented by the subcommittee says that the data collected should be highly relevant and it says that twice and my problem is with highly. It clearly ought to be relevant because if it's not relevant it has no benefits, but I don't know how to figure out how relevant it is other than by assessing the benefits. And just saying it has to be highly relevant up front seems to short circuit that process. How relevant it is, ought to be a conclusion and it also ought to depend on how intrusive it is. Something that is somewhat but not highly relevant but minimally intrusive may make sense because it may be better than other alternatives. And the saying it has to be relevant makes perfect sense. Saying it has to be highly relevant sort of prejudges that tradeoff and I think that's the point of the analysis.

Ms. Sotto: Jim.

Mr. Harper: I agree with the first amendment that Howard proposes. I think that the sentence flows better and to the extent it does what he wants as far as how it expresses the important parts of that sentence, I think that's fine. On the two highly's in the collection limitation and purpose specifications sub-bullet, I don't feel strongly one way or the other but I want to be cautious about that because I think we want to set a relatively high bar. I noted because I've been kind of contemplating this overnight that Herb Lin said this morning, and I don't remember what the context was, he said this morning, from a security standpoint everything might be relevant. And so a relevance standard is low enough, although there are other modifiers in the sentence, the relevance standard is low enough that you might be saying, you know, do whatever you feel like you want to do as far as keeping data. So that's a weak -- again, I don't feel strongly about it, but that's a weak note of caution about this amendment and I think further discussion will help me decide what I think about it.

Ms. Sotto: Mr. Hoffman.

Mr. Hoffman: You know, I think the -- I think in the nature of an approach that's based on trade-offs, it doesn't, you know, I think because the information collection does have some intrusion on this value and that's what it says if it's not relevant, you know, I think that is surfaced for the trade-off and that's the point of the analysis. It's not enough that all information could have some relevance. The whole point of the efficacy assessment, which I think is a key part of the story here, is you got to think about how much value there really is. And that I think is the real protection against the fishing expedition not the statement that it has to be highly relevant. I mean, I'm sort of I guess thinking of this against the backdrop of, if you will, credit scoring kinds of models where there's a lot of information that's relevant and if you had to decide a priori what was highly relevant before you did the analysis to figure out what really was important to making the assessment that you wanted to make, I'm not sure you'd get the same answer and I'm pretty sure you wouldn't get the best answer as to what information was useful for that result.

Ms. Sotto: No further discussion? Okay. I think we can take both, all three amendments together. Would anybody like to make a motion to accept the amendments?

Mr. Beales: I would.

Ms. Sotto: Mr. Beale's motions. Ramon seconds. All in favor. [A chorus of ayes]

Ms. Sotto: Any opposed? [No response].

Ms. Sotto: Thank you very much. Mr. Hoffman, did you have another point?

Mr. Hoffman: Yeah, this is not an amendment, it's a comment. I believe after having reviewed the framework many many times now with Jim and Joanne that this is going to be a very helpful document particularly to my subcommittee. We've talked about it internally as a subcommittee to the extent that this will be able to assist us as we're looking into our work which I'll describe in a few minutes. The one thing though I wanted to just confirm my -- state my understanding and make sure it's confirmed is that while I think the expectation is that we all are looking at this framework to help inform our analysis, I believe also our expectation is that this does not change in any way or is not a recommendation to the privacy office to change their currently existing processes focusing around the privacy threshold analysis and the privacy impact assessment as their main process for analyzing programs and new technology within the department but instead may be a useful tool to review those privacy impact assessments in light of to help inform the understanding of the issues.

Mr. Harper: Confirmed. I don't think we had any contemplation of trying to effect the privacy office's processes in putting this document together. It is written as Howard articulated so well, it is written in a way that may add to anyone's work when they're working on these issues as we say in the final sentence of the introduction. It may also in the optional may be useful to the privacy office, other DHS components, and other governmental entities that are seeking to reconcile personal data intensive programs and activities with important human values. So anyone wants to use, use it but by no means mandatory on anyone.

Ms. Sotto: Thank you. I have an additional point for discussion I think rather than amendment but possibly an amendment. The definition of privacy which is footnote one is attributed to Alan Westin. It is an early definition as it says here, 1967, the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. That seems to me to be a control, a definition that involves control of information which is very difficult, if not impossible I think in the homeland security context. I would hope that this definition as it stands from 1967 would not be sort of taken as any kind of definitive definition. And I think privacy is an incredibly difficult concept to define and in fact if we try to put parameters around the definition of privacy, we may in fact limit both our charge and the charge of the privacy office at DHS. I'd like to hear some discussion around this definition as used here in the footnotes. Joanne.

Ms. McNabb: Actually it's interesting that you bring that out. This document doesn't -- that's an aspect of the privacy interests so that definition of privacy then confidentiality, anonymity, seclusion, fairness, that isn't presented as the all-inclusive definition of the interests and privacy that ought to be reviewed. So while that's narrow, that's just one aspect.

Mr. Beales: I agree with Joanne. I think the, again, I think it's a strength of this document that it identifies the different interests. I think control is part of that but it's not the only answer. And if you lose some control but gain more of confidentiality and anonymity and seclusion, well that may be a gain from a broader privacy perspective. And I think the strength here is that breadth and so I don't have any problem with identifying the control interests and I think calling it privacy in the classic Westin sense is a fine way to do it. It certainly is a conventional way that it's used.

Ms. Sotto: Thank you. I'm comfortable with it. I'm particular comfortable with it saying that this is the Westin formulation and not trying to state that that is in fact the fixed definition of privacy. Ramon.

Mr. Barquin: I would just like maybe Maureen or someone from the privacy office to just refresh our memories and tell us what the privacy definition in..... [Laughter].

Ms. Cooney: Thank you. I don't know that I'll justly define privacy but what I would say is I would indicate some concern in the same way that Lisa has that the definition, at least in the way that it's written there, to a reader who first picks up this document and actually I saw the last draft where there was more text describing more on what privacy might be termed as, I believe that that's what I saw in the office. In any case this does seem too only be about control rather than other interests in privacy as well so it just seemed a bit narrow, particularly when in the government context, often people do not have choices on how their information is controlled. So I'm just not sure it was easily.....

Ms. McNabb: And that's why your office exists.

Ms. Cooney: Yes.

Mr. Harper: These are all interesting comments and one of the things that I think is important for everyone to understand, but especially us, is that DHS programs and law enforcement and commerce all rely on some diminution of privacy in order to work. And so the thing I wouldn't like us to do is say well we've approved all the information sharing that's happened so your privacy hasn't been impacted. It's a subtle but important distinction and I wouldn't want the language that we use or that is used to talk about these things to descend into where people are told well you have privacy because this is a fully approved program for taking and using your information. There are appropriate diminutions of privacy and I think by talking about the control dimension we're in a position to accurately talk about what's happening. You're losing some control over data and you're getting back a more secure country for it.

Mr. Hoffman: Jim, as I'm listening to the discussion and hearing Maureen's comment in particular, what do you think about sort of flipping the concepts, that the value identified in the bullet would be control and the text in the footnote would say this is the classic definition of privacy? I mean, the text in the footnote would be basically the same.

Mr. Harper: Taking that as an amendment to strike the word privacy at the beginning of the privacy bullet and calling in control?

Mr. Hoffman: Yeah. I'm on page four of eight, the bold privacy would be replaced by control.

Ms. McNabb: As an aspect.

Mr. Hoffman: As an aspect of privacy because the whole thing is about privacy and related interests and the, well actually and in the bold in the footnote would just change privacy to control as well and leave the text of the footnote exactly as it is, that this was the classic early definition of privacy.

Ms. Sotto: I would note that under that bullet as sub-bullets are confidentiality, anonymity, freedom from surveillance or whatever we changed, yeah, collection, limitation use, limitation retention, limitation, so I'm not sure.....

Mr. Hoffman: I withdraw that as an amendment.

Ms. Sotto: Lance.

Mr. Hoffman: Yeah, the problem we're having here for those of us who go back a ways is we're trying to code at the keypunch. [Laughter].

Mr. Hoffman: And there's a reason some of these are problematic, they're legitimate questions that have been raised, because these are concepts that not everybody agrees on as we've heard in the testimony and we all know ourselves. I suggest rather than trying to tweak one or two definitions it might make more sense to address especially Lisa's concern and that of others is to put an over-arching sentence or two at the head of the notes that says for purposes of reference or whatever here are some definitions, they're not the only definitions, there are trade-offs, yada, yada, but they are -- I wouldn't even say commonly accepted, but good enough that you can deal with. I don't have the exact words for it obviously but it would say this isn't the only definition of privacy or of surveillance or of liberty but they're close enough and I think that might get Maureen, for example, the running room she'd rather have and we wouldn't be doing violence to either our own thoughts or, you know, Alan Westin's in 1967. He by the way has four more definitions all in the same paper since then but, you know, it just depends.

Ms. Sotto: Reed.

Mr. Freeman: Well, in terms of mechanics and building on Howard's point with which I'm very close to agreeing with I think we could probably make everybody happy by on page four striking the bold word privacy and have it say control. And then in footnote one replace the bold word privacy with control and have it read, in Privacy and Freedom, Alan Westin formulated a classic early definition of privacy, then add in terms of control colon. Then we're -- we have it in there, we haven't made too many changes but we've said out loud that this is a definition that relates to control and we don't seem to be defining privacy in an overly narrow way.

Ms. Sotto: I think that the one problem with striking the word privacy on page four is that under that value fall all of the others up to fairness that come on page five and I don't think that those sufficiently serve the control bullet.

Mr. Harper: Lisa, I think on further consideration I think the sub-bullets actually are sub-bullets of privacy in the control sense and so they are suitably control so I think as Reed has proposed it and originally Howard I think that's actually all right.

Ms. Sotto: The collection limitation, use limitation, and retention limitation. How do you see those as control?

Mr. Harper: Well, the collection of the information in the first place deprives someone of control. Limiting your use post-surveillance reduces the amount that they've lost control. They have -- you're doing less damage to the control version of privacy when you carefully cabin your use of data after it's been collected. So I think it all works. I think it's all consistent.

Mr. Wright: I would agree that the structure of the document would fit if we changed the word privacy to control. I think the structure continues to make a great deal of sense so I think Reed has and Howard previously have come up with a change which adds some improvement to the document.

Ms. Sotto: Joe.

Mr. Beales: I mean, I think one of the problems we get into with the I guess the last minute word-smithing is the potential consequences in the words we choose without having time to think through them. I mean, I don't think there's necessarily anything in the document as is that can't pass muster for going down the pike and being amended in progress over time as a living document. So I would have a greater comfort in saying we all had an opportunity to have a long amount of comments at a specific point in time, we've agreed to a couple of amendments, I think this one has greater implications because one of the things that happens is when you change control to that framework, it seems to presume that you have a control over all of your privacy and all of your information which does not reflect any of the real world. When I walk down the street I do not have control over all of my personal information. People observe me. I am not secluded when I am walking through -- I'm not going to let that one go..... [Laughter].

Mr. Beales: You know, I'm observed. I don't have control over that and then all of a sudden to say everything is a parameter of control creates a facet that doesn't exist. So I think I understand why people have trouble with control as the only part of the definition. I agree that for the purposes of what we're using, control is the operative context in the definition of privacy but I think we may have unintended consequences like was the same concern with the modification on anonymity where anonymity is not an absolute. There are some places where you are not anonymous so I think that I would have a problem with control being given that kind of blanket status. I don't have a quick fix one-word solution but I also don't think, you know, using Alan Westin's definition puts us in dire jeopardy of being tremendously misunderstood since Alan Westin's definitions of privacy are quoted ad nauseam all over the place. So, you know, I think that's something that maybe we put in our minds and say as we go into the document and we look at your visions perhaps we can find better language to articulate these concepts to avoid confusion. You know, I think since this is a document whose primary purpose is to help us inform ourselves, we got the picture. [Laughter].

Mr. Beales: You know, I think other people who may use them if they read the minutes they now have essentially the, you know, the legislative history to the language now, they understand the problem, and I think I'd rather not create a new problem.

Ms. Sotto: Thank you. I will just remind this committee that this is the only forum in which we can all discuss these terms together so I think it's useful to do that, at least to some extent. Kirk.

Mr. Herath: I agree strongly with Joe. I think at a certain point we had pencils down here- [Laughter]

Mr. Herath: - and I think that any one of us if we were to go off into seclusion which I don't care for either but I, not that much- [Laughter]

Mr. Herath: I think we could come up with different ways of saying this probably 20 different ways. So I think that in the spirit of this being a living document and the fact that I don't think there's anything in here that's confusing to me, I'd say we go ahead and pass it. I agree with Lance. I mean, my I use don't let the good, you know, the perfect be the enemy of the good, all the time with my staff. I mean, at a certain point it becomes over-determined.

Ms. Sotto: Are there any other comments before we move on?

Mr. Beales: I was going to move to adopt the document as amended by the two amendments we did approve.

Ms. Sotto: I'll second. All in favor. [A chorus of ayes].

Ms. Sotto: Any opposed? The framework document is adopted with its two amendments. Congratulations and thank you. All right. If we could move on, please, to the date sharing and usage subcommittee. David Hoffman chairs that subcommittee. Would you give us a status report, please. SUBCOMMITTEE REPORTS: REPORT, DATA SHARING AND USAGE SUBCOMMITTEE

MR. Hoffman: Absolutely. The data sharing and usage subcommittee is working on three different areas of work currently. The first area is continuing our work on commercial data. We had published a paper that we continue to look for input from the public on that is posted to the committee's website on the use of commercial data to drive down false positives and when we did that we said that we would be working on a greater paper on the overall issues associated with the use of commercial data. We are working on that and the work is developing. And right now our intermediate goal is to get a fleshed out outline together of the major points in this area and to get that to a point where we can provide that for public comment as we continue to work on the paper to make sure that it's as transparent a process as possible and that we're soliciting as much input as we can. And so that is a big piece of work that we're going to be doing between now and the June meeting. The second piece of work that we're doing is that the subcommittee believes strongly as I mentioned before that the privacy impact assessment and the privacy threshold analysis are fundamental mechanisms by which the privacy office can drive privacy protection and the privacy interests into the department. We are doing a review of both the process and particularly the trigger mechanisms for when an individual project will fill out either the threshold analysis or the impact assessment and the substance of the privacy impact assessment and we are looking to do a short paper on that. We have not begun the authoring of that paper but are still gathering information about both the process and the substance. The third piece of work that we have going on is taking a look at the use of personal information and the collection of personal information for disaster preparedness and in the event that a disaster happens. We are looking at that right now in general terms and the processes that are in place within the department to handle those issues and then there will be a document that we will author that will look at that issue with specific focus on the Katrina experience.

Ms. Sotto: Thank you. Are there any questions for David? Okay. Let's move on then to a report from the fourth subcommittee, the screening subcommittee, chaired by Howard Beales. SUBCOMMITTEE REPORTS: REPORT SCREENING SUBCOMMITTEE

Mr. Beales: The screening subcommittee is going to build on our secure flight recommendation. We are to take a more general look at screening programs and try to derive some more general principles and make some more general recommendations. The first step in that process is we're going to take a look at about six different screening programs to make sure -- I mean, we think we understand secure flight and the issues there pretty well at this point. We want to take a look at five or six other screening programs to see how they map and to make sure we've got a good sense of what the general issues are, and then use that to develop a general set of recommendations about how the department ought to think about screening programs in general. We're a little unclear about what our timetable is going to be because it depends on, you know, sort of one scenario is our work on secure flight means we've already thought of everything and we've figured out all the answers. That seems a little unlikely. The other scenario is there's huge amounts of additional work to do. Hopefully that's not too likely either but until we've taken a look at the other program, you know, it's not clear how close we'll be to having a recommendation. So I would hope that we would have substantial progress by June and something to adopt perhaps at the following meeting.

Ms. Sotto: Thank you very much and many thanks to all of our subcommittees and all the members of our subcommittees for all of their efforts and enormous, enormous amounts of time spent on these papers and the thinking behind them so deep thanks for that. We are now ready for our public comment period. Do we have any -- we have no public comments. None at all. Okay. With that, I would ask for a motion to adjourn, please. UNIDENTIFIED VOICE: So move.

Ms. Sotto: Seconded. Thank you. All in favor. [A chorus of ayes]

Ms. Sotto: Any opposed? [No response.]

Ms. Sotto: Thank you, the meeting is adjourned. [Whereupon at 5:00 the meeting was adjourned]